Individually Watermarked Information Distributed Scalable by Modified Transforms

Mr. K-G Stenborg
FOI Swedish Defence Research Agency
P.O. Box 1165
SE-581 11 Linköping
Sweden

kgsten@foi.se

ABSTRACT

Distribution of secret information in audio, video or images to known recipients are made secure by encryption. The weak part of such distribution scheme is after the decryption of the content, since if the media deliberately or by mistake is redistributed the cryptology no longer is effective. One way to discourage deliberate re-distribution is to embed the information with individual watermarks (sometimes called fingerprinting) for each recipient. If for example a copy of an illegally redistributed image is obtained the individual watermark can be retrieved and identify the re-distribution source. After the source is traced an investigation must be made to decide if the re-distribution was made deliberately or by mistake, or if the image somehow has been stolen from the original recipient.

The problem with distribution of individually watermarked information is that to distribute a unique content by unicast to each recipient requires a large bandwidth and much power at the distributor. This is especially apparent if the number or recipients are large. Therefore scalable methods, with a bandwidth need that do not expand drastically for even large number of recipient, are needed for distribution of individually marked content.

Previous methods for solving the scalable distribution problem either use special networks with active routers or split the content into a shared non watermarked part and a watermarked part. The watermarked part can be unique for each recipient or in part be shared with other recipients. All of these methods will need a larger bandwidth and complex embedding at the distributor or in the network. Another type of methods distributes the same content to all recipients but some type of descrambling is needed at the recipient to be able to use the content. During the descrambling the individual watermark is embedded. The method of Modified Transform Watermarking uses a type of scrambling caused by using modified transforms.

Individual watermarks must be able to restrain collaborating attacks when more then one individually embedded content is combined to try and remove the watermarked information. Ideally all copies that have been used in such an attack should be able to be retrieved for a robust watermarking method but for many applications it is enough that one of the used individual watermarks are identified.

1.0 INTRODUCTION

In networks that are dealing with secure information such as images, video or audio these media objects can be encrypted during transmission. But such an encryption may not prevent intentional or unintentional re-distribution from the original recipient to unauthorised persons or organizations. One method to discourage illegal re-distribution is individually watermarks that can be used to trace the source of illegally re-distributed media.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Individually Watermarked Information Distributed Scalable by Modified Transforms	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **FOI Swedish Defence Research Agency P.O. Box 1165 SE-581 11 Linköping Sweden**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADB381582. RTO-MP-IST-087 Information Management - Exploitation (Gestion et exploitation des informations). Proceedings of RTO Information Systems Technology Panel (IST) Symposium held in Stockholm, Sweden on 19-20 October 2009

14. ABSTRACT

Distribution of secret information in audio, video or images to known recipients are made secure by encryption. The weak part of such distribution scheme is after the decryption of the content, since if the media deliberately or by mistake is redistributed the cryptology no longer is effective. One way to discourage deliberate re-distribution is to embed the information with individual watermarks (sometimes called fingerprinting) for each recipient. If for example a copy of an illegally redistributed image is obtained the individual watermark can be retrieved and identify the re-distribution source. After the source is traced an investigation must be made to decide if the re-distribution was made deliberately or by mistake, or if the image somehow has been stolen from the original recipient. The problem with distribution of individually watermarked information is that to distribute a unique content by unicast to each recipient requires a large bandwidth and much power at the distributor. This is especially apparent if the number or recipients are large. Therefore scalable methods, with a bandwidth need that do not expand drastically for even large number of recipient, are needed for distribution of individually marked content. Previous methods for solving the scalable distribution problem either use special networks with active routers or split the content into a shared non watermarked part and a watermarked part. The watermarked part can be unique for each recipient or in part be shared with other recipients. All of these methods will need a larger bandwidth and complex embedding at the distributor or in the network. Another type of methods distributes the same content to all recipients but some type of descrambling is needed at the recipient to be able to use the content. During the descrambling the individual watermark is embedded. The method of Modified Transform Watermarking uses a type of scrambling caused by using modified transforms. Individual watermarks must be able to restrain collaborating attacks when more then one individually embedded content is combined to try and remove the watermarked information. Ideally all copies that have been used in such an attack should be able to be retrieved for a robust watermarking method but for many applications it is enough that one of the used individual watermarks are identified.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**10**	

In this paper we have chosen to have a general description concerning what type of network and scenario that is used. It could be a network of surveillance cameras transmitting to a security central, distribution of maps to trusted parties, radio communication or distribution of visual/IR video between vehicles and soldiers. The transmission could be live sent or accessed from a stored media database. Most of the methods described are adapted for broadcast type of distribution to a large number or recipients but we will also discuss how these methods can be used in other distribution situations.

2.0 WATERMARKING

Digital watermarking [1] can be used to embed a watermark in digital media, figure 1(a). The watermarked media should not contain any notable distortion caused by the watermark, i.e. a watermarked image should not be perceptually different from the original unmarked image. The embedded watermark can be extracted from the watermarked media object. In some methods the original media is needed for the extraction, figure 1(b), and other methods can extract the watermark without any knowledge about the original media, figure 1(c).

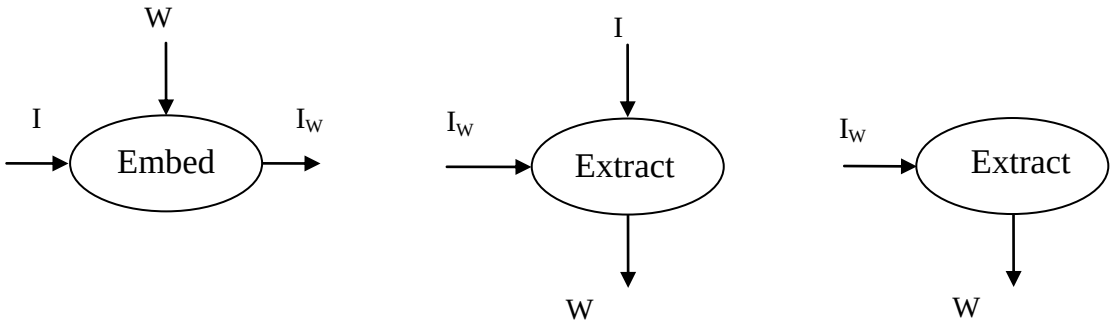

Figure 1: (a) Embedding the information I with the watermark W creates I_W. (b) Extraction of W from I_W is done with information from I. (c) Extraction of W from I_W is done without any information from I.

These embedded watermarks can be of different types used for varying types of purposes. Three of the most common types of watermarks are:

- Fragile watermarks can be used to check if the media have been altered or if it still is identical to the original form.
- Robust watermarks can contain information about the media such as a timestamp, position, security classification and ID of creator.
- Robust individual watermarks can be used to trace the source of a redistributed copy of a media object. Individual watermarking are sometimes known as Fingerprinting.

For many cases two or more types of watermarks can be embedded in the material independently from one another. In this work we will concentrate on the last type with robust individual watermarks. A scenario for this method is a distribution system where more than one node has access to the media. These nodes can be persons or locations in the distribution net. Let the media be an image and the nodes be persons. For each person, the image that he has access to will contain an individual watermark associated with him. Such an individually watermarked copy is by some reason (intentional or unintentional) redistributed in a prohibitive way. If an illegal copy is obtained, the individual watermark can be retrieved and identify the source of the re-distribution.

For the watermarking algorithm to be considered robust, the embedded watermark should be able to be extracted and identified even if attacks are performed on the media object. For an image, attacks can be unintentional such as lossy compression or distribution errors, or the attacks can be done deliberately by the person responsible for the re-distribution. Deliberately attacks can for example be cropping, adding noise, quantization or rotating the image. If two or more persons are collaborating they can try to remove the watermarks by somehow combining their individually watermarked copies. One such *collaborating attack* is to take the mean for each pixel from an image, or by randomly using the value from copy 1 or 2 for each pixel.

3.0 DISTRIBUTION

Distribution of media object can be done in many different ways. Traditionally IP-packets are distributed by unicast, multicast or broadcast [2]. Networks for distribution of information can either have one distributor or many distributors. In a similar way they the network can have one or many possible recipients.

3.1 Four distribution models

The distribution of information such as media can be done in many different ways dependent on the structure of the network. For media that is only distributed in one step (with nodes either being source nodes or recipient nodes) four different types of networks exist:

1. One source node distributes media to one recipient node.
2. One source node distributes media to more than one node.
3. More than one source nodes distributes media to one recipient node.
4. More than one source nodes distributes media to more than one recipient node.

For distribution with more than one recipient node individual watermarking can be used so that the recipient get individually marked copies. For the first case (figure 2) with only one recipient of the media, a watermark containing the identity of the source might be enough to also identify the recipient. If such a copy is redistributed the question may arise whether the recipient is responsible or if the source node in some way might be guilty. To eliminate such concerns a watermark should be embedded at the recipient node so that any redistributed copy will contain information about whether it originates from before it was distributed to the recipient or after.

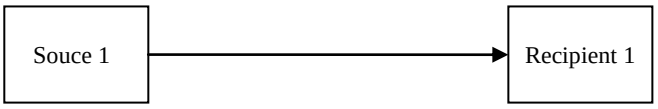

Figure 2: Distribution from one source node to three recipient nodes.

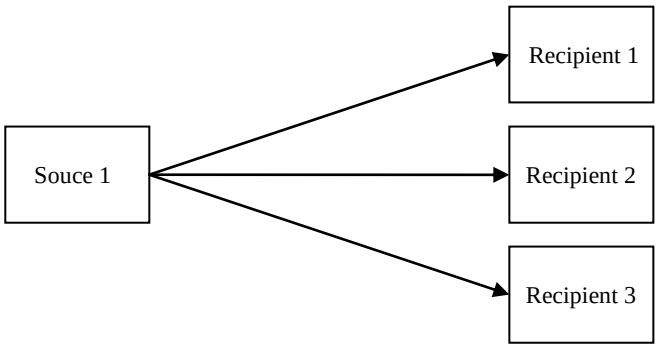

Figure 3: Distribution from one source node to three recipient nodes.

In the second case, with one source and many recipients, the individual embedding can be done in a number of places during the distribution, figure 3. The individual watermark can be embedded at the source node and then be distributed in a secure way to each. Such a distribution will be very bandwidth costly and if the distribution channel is not considered to be a 100% secure it will be uncertain whether the recipient is guilty of any re-distribution or whether such copy might have been retrieved before it reached him. The individual watermark can also be embedded in the network or at the recipient.

The third case with many distributors and only one recipient can for example be a security central connected to many surveillance cameras. In many ways this network case can use the same methods that are applicable for the network in case one. For this and all other networks with more than one distribution node a watermark containing the source ID can be embedded (independent from the individual watermark) so that the source can be identified.

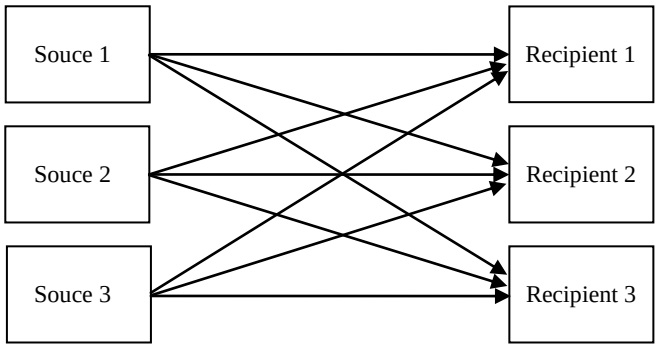

Figure 4: Distribution from three source nodes to three recipient nodes.

For the fourth case with many source nodes and many recipients, the complexity will increase for network embedding systems, figure 4. This can for example be number of operators that have access to the same remote sensors. This is the most general case for the single distribution networks.

3.2 Allowed re-distribution between recipients

For a system that allows the recipient nodes to re-distribute the media to other authenticated recipient nodes in the network the distribution scheme becomes more complex. The original recipient can now be one of the source nodes given in the four network cases above. Such a distribution system for case 1 is given in figure 5.

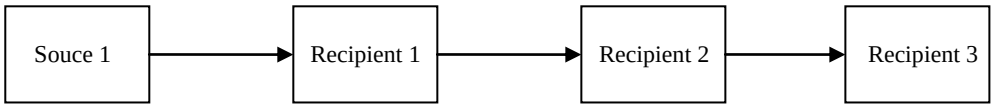

Figure 5: Recipient node 1 re-distributes the media originating from source 1 to authenticated recipient 2 who in turn distributes the information to recipient 3.

The handling of the individual watermarks becomes more complex for networks with recipient nodes that can act like source nodes. Given the example in figure 5 the media at recipient 1 contains an individual watermark identifying that recipient. After the allowed re-distribution to recipient 2 the individual watermark should identify recipient 2 (and possibly also give information about the previous distribution chain with recipient 1). Since recipient 1 is also a distributor and some individual watermarking methods use embedding at the distributor, recipient 1 should be able to embed the individual watermark identifying recipient 2 for that type of watermarking methods. But that means that any recipient would be able to embed the individual watermark of any other recipient and therefore the individual watermarks can no longer be used to identify which recipient that preformed a re-distribution to non authenticated recipients. Therefore the individual watermarking can not be performed at the re-distribution source. Instead this can be done in the network or at the new recipient. A special case of network embedding would be to have an intermediary node that embeds the individual watermark, see figure 6. Such an embedding node could also be used to check if the re-distribution from recipient 1 to recipient 2 is allowed, i.e. if recipient 2 are authenticated for the given media object. The embedding node can also be used during the original distribution from source 1 to recipient 1. The embedding node can either be a single node that handles all embedding during distribution or the system can be built with many unique embedding nodes that handle one recipient each.

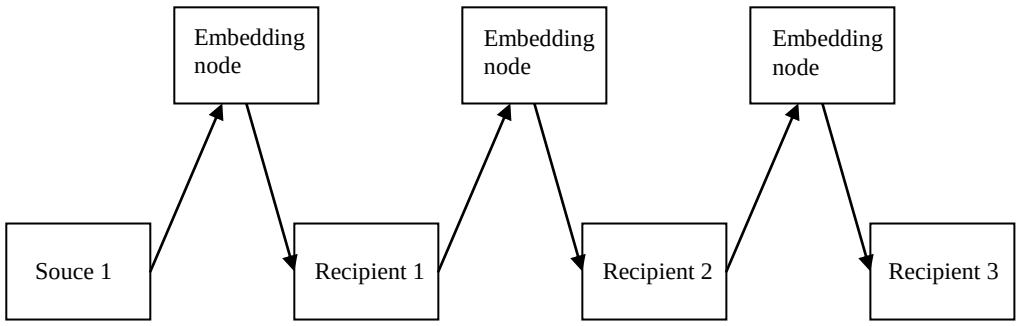

Figure 6: Source 1 uses the intermediary embedding node to create the individual watermark during distribution to recipient 1. Recipient 1 also uses a embedding node during distribution to recipient 2.

So far we have only discussed the source nodes and the recipient nodes but many networks also contain relay nodes in the network (routers). Some of the methods that are described in the next section will use such nodes.

4.0 INDIVIDUALLY WATERMARKED CONTENT DISTRIBUTION

For individual watermarking to be included in a distribution system the cost of the embedding should not be larger than the gain given by the added feature. The cost can be measured by:

- Bandwidth increase cased by the embedding
- Speed decrease during distribution cased by the embedding step
- Flexibility to expand the distribution system
- Monetary cost

Previous research in this area has mostly dealt with distribution from one distributing node to a large number of recipients. Below we will look at some of these methods and comment on their use for other type of distribution cases. All of these watermarking methods can be describes as belonging to one of five different categories: Source Based Watermarking, Network Based Watermarking, Unique Fragment Watermarking, Shared Fragment Watermarking and Client Based Watermarking. Most of these methods rely on decryption to get a secure transmission between source and recipient.

4.1 Source Based Watermarking

In this category are employed the simple method of embedding the individual watermark at the source for each receiver and transmit each such watermarked copy to its recipient. This method is not bandwidth efficient since the media has to be transmitted once for each recipient. As mentioned earlier such a watermarked copy will not tell if the re-distribution has happened before or after the recipient received it since the watermark is already implemented during the initial distribution.

4.2 Network Based Watermarking

The methods in this category use specially constructed networks that embed the individual watermark during transmission.

A method known as WHIM [3] uses a tree structure network and a multicast/broadcast type of distribution. Each node in the network embeds its unique watermark ID during transmission of the media. By doing so it will be possible to extract all of these watermarks and trace the transmission chain from the source node to the recipient node. In the last node before the recipient the embedded watermark can also contain the ID of the recipient. A similar method called Hierarchical tagging is described in [4].

These two types of watermarking can also be used for more than one distributing node and also for allowed re-distribution. But it will only work for networks with a number of nodes between the source and recipient. A network that directly connects the source and recipient can not be used. Another problem is that the constant embedding by the nodes will slow down the transmission and that the media must be able to carry many watermarks.

Another network based watermarking method is called Watercasting [5]. It is also based on a tree structure network with intelligent nodes that distributes the information. The information of the media object is divided into a number of packets during transmission. At the source node the information for each packet is made into a number of copies embedded with different watermarks. These embedded packet copies are

transmitted to the network. The intelligent nodes in the network forward all but one of these packet copies to the following nodes. Which packet copies that are not transmitted further depend on the nodes and the forward structure is changed for each new group of packet copies. The combined information from the received packets at the recipients contains individual watermarks.

A disadvantage with this method is that a larger bandwidth is needed at the beginning for the copies of each packet. The forward distribution structure must be saved for a recipient to be traced given a watermarked object. If more than one source node is active the forward distribution structure will become complex. Since the individual watermark is built from many packets during the distribution any allowed re-distribution would probably remove the original individual watermark. If the original watermark remains it would mean that each packet contains two watermarks and to trace the transmission route given that might be impossible. Therefore this method is not suitable for many network types. As for WHIM and Hierarchical tagging this method can only be used in transmission systems with active nodes between the source and recipients.

4.3 Unique Fragment Watermarking

Methods in this category split the distributed information in to two parts, first one general part that is shared among all recipients and then one recipient specific part that is individually embedded and distributed to each corresponding recipient. Since the embedding is done at the source node these methods also belong in the Source Based Watermarking category. Methods that use this type of distribution are described in [6] [7] and [8]. The specific part of the information should contain the most important parts of the media. It should not be possible to reconstruct the media object by only using the information in the general part.

For a large number of recipients these types of methods still need a large bandwidth but for a limited number of recipients they can be useful. Once again the watermark will not contain information about whether it has reached the recipient or not since all the watermarking is done at the source. For allowed re-distribution networks a great choice would be to use embedding nodes that can embed individual watermarks in the recipient specific part while the general part can be distributed freely from one recipient to another.

4.4 Shared Fragment Watermarking

The methods in his category do not have any individual distribution to the recipients. Instead each recipient will build a media object from watermarked information fragments. At the source these fragments are made into two or more copies that are embedded with different watermarks. Similar to Watercasting all such fragment copies are distributed. Each fragment copy is encrypted with different keys and the recipients are only given one decryption key for each fragment copy. The set of decryption keys are unique for each recipient. Therefore the information that is made from the decrypted fragments at the recipient contains an individual watermark. The information can be IP packets [9], frames in a video stream [10] or blocks of an image [4].

The methods in this category needs less bandwidth for large number of recipients compared to last category. One challenge for these methods is collaborating attacks with the information fragments of two or more recipients blended. These methods do not seem to be able to be adopted for allowed re-distribution networks by any simple means.

4.5 Client Based Watermarking

Another category of methods distribute the same content to all recipients but the information is scrambled by some means at the source node. The recipients must descramble the content to be able to use the

information. To descramble the information a recipient individual key (or hardware) is used. During the descrambling the individual watermark is embedded. The descrambling and embedding can be combined using slightly different decryption keys [11] [12], adding of an individual mask [13] or by letting each recipient only be able to decrypt the sign of some encrypted transform components [14].

The methods in this category do not transmit any redundant data such as copies of packets. Therefore the needed bandwidth will be lower compared to them. Another great advantage is that the embedding is done at the recipient. Thereby it can be established that information containing an individual watermark has reached the recipient.

5.0 MODIFIED TRANSFORM WATERMARKING

Our watermarking method Modified Transform Watermarking [15] belongs in the Client Based Watermarking category since the same content is distributed to all recipients. The content is scrambled during distribution so that a descramble key is needed for the recipient. Each recipient has an individual descramble key. The individual descrambling is made in such way that the original content is not fully restored. Instead a small individual noise is embedded in the information – the watermark. The noise should not be visually noticeable in images or video. So far our method has only been adapted for visual and not audio content. Below we will only talk about watermark distribution of still images. The distribution of an image is given in figure 7.

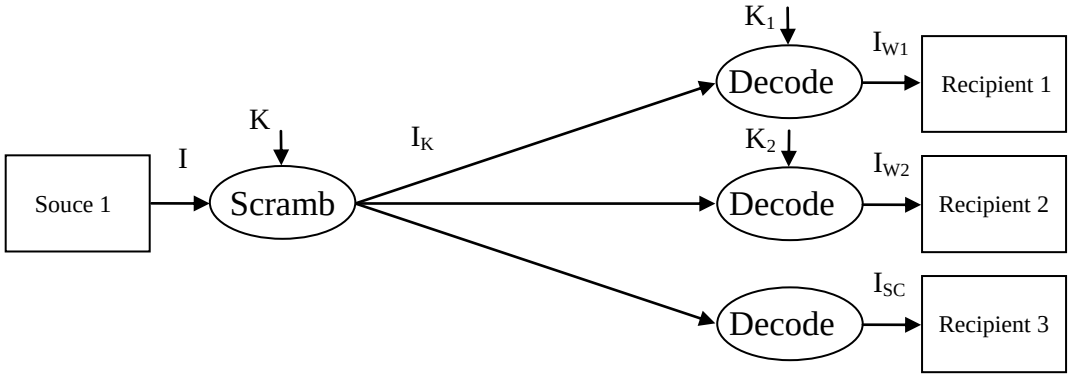

Figure 7: Distribution using Modified Transform Watermarking. The image I is transformed using the key K at the source. Recipient 1 uses his unique descrambling key K_1 to decode the transformed image and gets the individually watermarked image I_{W1}. Recipient 3 tries to decode the transformed image using an ordinary decoder and gets the heavy scrambled image I_{SC}.

While other methods embed the watermark in the spatial or frequency domain our method is embedded during the transformation from one domain to the other. At the distributor the image is transformed with a secret transform (somewhat based on the DCT - discrete cosine transform). If an ordinary IDCT (inverse discrete cosine transform) transform is used to try to reach the spatial domain the result is a heavily distorted image, i.e. the scrambled image. To reach the original image the inverse of the secret transform is needed. Each trusted recipient has a unique inverse transform that is similar to the inverse of the original transform. The elements of this individual inverse transform are given by the individual descrambling key. After applying the individual inverse transform the retrieved image is embedded with a recipient individual watermark.

The transforms are chosen so that if the elements of more than one key are used to create a new key the resulting image after the descrambling contains enough watermark information to trace the used keys. Similar, if more than one different descrambled image is combined in a collaborating attack the resulting watermark will still identify which images that have been used.

Since the image is transformed during the transmission between the source and the recipient it is very compelling to use the transform as a first step in an image encoder. Usually in transformation coding the DCT transform in combination with quantization and source coding is used to achieve lossy compression. Instead of applying the secret transform on the whole image we can use blocks of 8x8 pixels similar to DCT transform coding. This gives the possibility to use different secrets transforms for the different blocks. In that case the recipients need to have a set of keys so that all the blocks can be descrambled. Our experiments show that by using the secret transform instead of the DCT during the compression we will get a slight data expansion of about 5%. Compared to many other of the watermarking methods mentioned before this is a very small expansion of the needed bandwidth.

If a recipient would like to re-distribute the image he can chose to transmit the scrambled image instead of transmitting the descrambled and individually watermarked image. If the recipient of the re-distributed image is not authorized he will not have access to any correct descramble key and will thereby not be able to descramble the image. In a similar way this method is suited for access by demand type of distribution with the media being stored at a server that the recipients can download when they need it. The server does not need to perform any embedding before the transmission since the media is already scrambled before it was stored.

6.0 CONCLUSIONS

Individual watermarked media can be used to trace illegally distributed information. The watermark will also discourage from prohibitive re-distribution. Many different types of distribution networks exist and finding a suitable individual watermarking method can be difficult. Especially if the recipients are allowed to share (re-distribute) the information with other authorized recipients in the network. One way of making such re-distribution easy to implement would be to use an embedding node that is always used during transmission. That node can both check to see that the intended recipient is authorized and embed an individual watermark before the information is transmitted further.

Previous methods for making distribution of individual watermarking easy have mostly dealt with large broadcast type of networks with one source node and many recipients. Some of these methods are more easily adapted to other types of networks and some are very limited to specific type of distribution schemes. Source Based Watermarking is the most simple type of method but can be used for smaller number of recipients provided that enough power exist at the source to embed and transmit all the individual watermarked media. The Network Based Watermarking methods are limited to specific type of networks. The Unique Fragment Watermarking methods is not suitable for large group of recipients but can be adopted to use embedding nodes to achieve allowed re-distribution. The Shared Fragment Watermarking methods on the other hand can handle large groups of recipients without increasing the needed bandwidth much but is not suited for re-distribution networks. Finally the methods in the Client Based Watermarking category are the most promising since they can handle large number of recipients, do not rely on any specific network and can be adopted for allowed re-distribution networks.

Modified Transform Watermarking is a Client Based Watermarking method that uses a secret transform to scramble the information before transmission. The information can not be used without the descrambling key that embeds the individual watermark and the method is robust against collaborating attacks. Since the method is similar to compression methods it will give a low bandwidth during distribution.

7.0 REFERENCES

[1] Cox, I. j., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). Digital Watermarking and Steganography – Second Edition. Morgan Kaufmann.

[2] Stevens W. R. (1994). TCP/IP Illustrated, Volume 1 – The Protocols. Addison-Wesley.

[3] Judge, P., & Ammar, M. (2000, June). WHIM: Watermarking multicast video with a hierarchy of intermediaries. In Proceedings of the International Workshop on Network and Operation System Support for Digital Audio and Video NOSSDAV'00, 39(6), 699-712.

[4] Caronni, G., & Schuba, C. (2001, December). Enabling hierarchical and bulk-distribution for watermarked content. In Proceedings 17th Annual Computer Security Applications Conference ACSAC'01, (pp. 277-285).

[5] Brown, I., Perkins, C., & Crowcroft, J. (1999, November). Watercasting: Distributed watermarking of multicast media. In Proceedings of the First International COST264 Workshop on Networked Group Communication NGC'99, (pp. 286–300).

[6] Wu, T-. L., & Wu, S. F. (1997). Selected encryption and watermarking of MPEG video. In International Conference on Image Science, Systems, and Technology CISST'97.

[7] Zhao, H. V., & Liu, K. J. R. (2006, January). Fingerprint Multicast in Secure Video Streaming. In IEEE Transactions on Image Processing, 15(1), 12-29.

[8] Luh, W., & Kundur, D. (2005). New paradigms for effective multicasting and fingerprinting of entertainment media. In IEEE Communications Magazine, 43(6), 77–84.

[9] Parviainen, R., & Parnes, P. (2001, May). Large scale distributed watermarking of multicast media through encryption. In International Federation for Information Processing Communications and Multimedia Security Joint working conference IFIP TC6 and TC11.

[10] Chu, H. H., Qiao, L., & Nahrstedt, K. (2002, April). A secure multicast protocol with copyright protection. ACM SIGCOMM Computer Communications Review, 32(2), 42–60.

[11] Anderson, R., & Manifavas, C. (1997, January). Chameleon - A new kind of stream cipher. In Proceedings of the Fourth International Workshop on Fast Software Encryption FSE'97 (pp. 107–113).

[12] Briscoe, B., & Fairman, I. (1999). Nark: Receiver-based multicast nonrepudiation and key management. In Proceedings of the First ACM conference on Electronic commerce (pp. 22–30).

[13] Emmanuel, S., & Kankanhalli, M. S. (2003). A digital rights management scheme for broadcast video. Multimedia Systems Journal, 8, 444–458. ACM-Springer Verlag.

[14] Kundur, D., & Karthik, K. (2004, June). Video fingerprinting and encryption principles for digital rights management. Proceedings of the IEEE, 92(6), 918–932.

[15] Stenborg, K-G. (2009). Scalabale Distribution of Watermarked Media,. Handbook of Research on Secure Multimedia Distribution, Chapter 18, 335-351, Information Science Reference, IGI Global.